Procedure No.2205.09: Network Security
Reference: 2205
Effective Date: 12/28/04
Prior Issue: N/A

Purpose:

The Arizona Department of Juvenile Corrections (ADJC) establishes management direction, procedures, and requirements to ensure the appropriate protection of ADJC information is handled by computer networks. This procedure covers all computer and communication devices owned or operated by ADJC that routes, passes, or directs network traffic and covers any computer and communications device that are present on ADJC premises, but which may not be owned or operated by ADJC.

Rules:

1. **MANAGEMENT OF INFORMATION SYSTEMS (MIS)** shall protect the processing, storage, and accessibility of data through Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs). Protection of network resources will be based on sensitivity and value to the Department. Access to network resources (e.g. data, applications, etc.) is granted on a need-to-know basis. **MIS CHIEF INFORMATION OFFICER (CIO)** shall review a user's information needs before authorizing access.

2. The **ADJC NETWORK SECURITY TEAM** shall tightly control interconnection of computers and networks to the Internet and the ADJC network LAN/MAN/WAN. Department Personnel shall not authorize a direct connection of a network or circuit to other Agencies, business partners or Internet Connectivity through the ADJC enterprise firewall without pre-approval from the ADJC Network Security Team. **THIS TEAM** shall have the authority to mandate immediate network reconfiguration should an unacceptable risk situation arise or major technology shift occur.

3. Unauthorized access from the Internet into any portion of the ADJC network shall be prevented. **AGENCY PERSONNEL** wanting to offer public access to certain information shall ensure that machines dedicated to this purpose remain isolated from machines used to operate the ADJC's day–to–day business and from devices storing or containing non-public data.

4. **AGENCY PERSONNEL** shall report all suspected security violations to the ADJC Network Security Team at 602-542-0289 or e-mailed to NetworkSecurity@azdjc.gov . **AGENCY PERSONNEL** shall:
   a. Complete Computer Incident Response Form, Form 2205.09;
   b. Include in any communication as much information as possible about the time, error messages, and IP addresses involved in the incident. The **NETWORK SECURITY TEAM** shall coordinate trouble shooting and reporting with vendors, ADOA CERT team, and criminal investigation units, if necessary.

5. **ADJC USERS** shall treat all information traveling over the ADJC networks that has not been specifically identified as the property of other parties as though it is an ADJC information asset. ADJC prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, ADJC protects third party information that has been entrusted to the Department and in accordance with applicable contracts.

6. All routers and switches connected to ADJC's production networks are affected. Routers and switches within internal, secured isolated test labs are not affected. **MIS** shall ensure that every router meets the following configuration standards:

a. No local user accounts are configured on the router. Routers shall use TACACS+ or RADIUS for all user authentication;
b. The enable password on the router shall be kept in a secure encrypted form. The router shall have the enable password set to the current production router password from the router's support organization;
c. The following shall be disallowed:
   i. IP directed broadcasts;
   ii. Incoming packets at the router sourced with invalid addresses such as RFC1918 address;
   iii. TCP small services;
   iv. UDP small services;
   v. All source routing;
   vi. All web services running on router;
d. Corporate standardized SNMP community strings shall be used or have those disabled;
e. Access lists and rules are to be added as business needs arise;
f. The router shall be included in the corporate enterprise management system with a designated point of contact;
g. Each router shall have the following statement posted in clear view:
   i. "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You shall have explicit permission to access or configure this device by ADJC. All activities performed on this device will be logged, and violations will result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

7. **ADJC EMPLOYEES, CONTRACTORS, VENDORS AND AGENTS WITH REMOTE ACCESS PRIVILEGES TO ADJC'S CORPORATE NETWORK** shall ensure that their remote access connection is given the same consideration as the user's on-site connection to ADJC.
a. General access to the Internet for recreational use by immediate household members through the ADJC Network on personal computers is not permitted.

Effective Date:	**Approved by Process Owner:**	**Review Date:**	**Reviewed By:**